REMARKS

This Amendment is responsive to the non-final Office Action mailed March 24, 2008. This Amendment is accompanied by a Request for a Three Month Extension of Time, and by payment of the required extension fee for a small entity.

This application had been the subject of an Appeal to the Board of Patent Appeals and Interferences. Following briefing for the appeal, the Examiner returned this application to active prosecution, withdrawing the previous final rejection, and modifying the basis for the Examiner's rejection of the pending claims.

The claims that are currently pending in this application are claims 184-189, 191-213, 215-229, 231-234, 236-243, 248-255, 258-271, 279, 327-340, and 346-348.

There are a total of seven pending independent claims, namely, claims 236, 248, 252, 258, 260, 264, and 268. Each of these independent claims has been amended above. Applicant did not intend to amend any of the pending dependent claims above.

Rejection of Independent Claims 236, 248, 252, 260, 264, and 268

The Examiner has set forth the basis of the rejection of independent claims 236, 248, 252, 260,264 and 268 in Paragraph No. 3 of the Office Action, which bridges pages 2, 3 and 4 of the Office Action. The Examiner has rejected each of these independent claims under 35 U.S.C. §103(a) based upon U.S. Patent No. 6,629,131 (Choi) in view of U.S. Patent No. 6,618,747 (Flynn) and U.S. Patent No. 6,836,846 (Kanevksy).

The Examiner notes, on page 2 of the Office Action, that Choi does not disclose: 1) detecting an access event; 2) prompting the party associated with said event to input recipient data related to the party associated with said requested access; or 3) sending recipient data for confirming proper delivery of said e-mail. On the other hand, the Examiner states that Flynn discloses: 1) detecting an access event; 2) discovering a stored data file associated with the actual recipient's e-mail address; and 3) sending identifying data contained in said discovered data file for

confirming proper delivery of the e-mail. The Examiner contends that it would have been obvious to modify Choi in accordance with Flynn to incorporate the "detecting", "discovering" and "sending" features summarized above.

The Examiner further notes, at page 3 of the Office Action, that neither Choi nor Flynn disclose the use of biometric information to identify the recipient. The Examiner states that Kanevksy discloses the use of biometrics to identify the recipient. The Examiner argues that it would have been obvious to combine the use of biometrics, as disclosed by Kanevsky, with Choi and Flynn, in the manner claimed by Applicant within claims 236, 248, 252, 260,264 and 268.

As a preliminary matter, neither of the independent claims 236 or 248 recites the use of biometrics to identify the recipient. Accordingly, Applicant does not understand why the Examiner included claims 236 and 248 within the group of claims rejected in Paragraph 3 of the Office Action, nor why the Examiner felt it necessary to add the Kanevsky reference to Choi and Flynn in order to reject claims 236 and 248. Nonetheless, Applicant will address the Examiner's rejection of such claims as presented by the Examiner within paragraph 3 of the Office Action.

Claim 236

Claim 236 as amended sets forth a method for verifying whether an e-mail received by a recipient was accessed by an intended recipient. The recited method includes the step of "detecting an access event, and prompting the party associated with said access event to input recipient data prior to allowing the requested access". Claim 236 also states that the "recipient data" (which the recipient must input before being allowed to access the e-mail message) includes "identifying data related to the party associated with said requested access". In addition, claim 236 recites the additional step of "permitting said e-mail to be accessed after the party associated with said access event inputs said recipient data". Claim 236 further recites the step of sending "identifying data relating to the party associated with said access event ... to identify the party who accessed said e-mail".

As mentioned above, claim 236 includes the step of "prompting the party associated with said access event to input recipient data prior to allowing the requested access". The Examiner argues in the Office Action that Flynn discloses "... discovering the stored data file that is associated with said actual recipient's e-mail address". However, claim 236 does not recite a step of discovering any stored data files. Rather, claim 236 recites the step of prompting the party associated with the access event to input recipient data prior to allowing the requested access.

Flynn discloses a system wherein an intended recipient is notified that an email message has been posted at a third party web host for such recipient. Notification of the existence of the posted e-mail is communicated by the third party web host which sends an e-mail message informing the recipient that an e-mail message is waiting for the recipient at a specified third party web host URL. Included in this e-mail message is the third party URL address where the posted message is located. If the intended recipient accesses the message, a confirmation notice is sent to the sender to confirm that the message was downloaded. Flynn describes the URL address at which the posted e-mail message is posted on the third party web host as a "unique call address" (assigned by Flynn's Web Server 24) that provides access to an e-mail message stored at such unique call address on the third party Web server. When the email message is downloaded by the requesting party, Flynn's system sends a confirmation of receipt notice that includes the address to which the email was downloaded, the time it was downloaded, and optionally, a compressed copy of the original message.

The Examiner does not contend, within Paragraph 3 of the Office Action, that Flynn prompts a recipient to input recipient data before permitting access to an e-mail message, as required by claim 236. Indeed, Flynn does not prompt a recipient to input any recipient data that identifies the recipient. Flynn merely allows a requesting party to access the message, notes the email address to which such message is downloaded following such request, and notifies the sender of the email address to which such e-mail message was downloaded.

Therefore, the arguments raised by the Examiner in Paragraph 3 of the Office Action fail to support the Examiner's rejection of claim 236 for obviousness based upon Choi, Flynn and Kanevsky.

Claim 248

Claim 248 recites a system for verifying whether e-mail received by a recipient was accessed by an intended recipient, the system including a recipient computer connected to a communications network and capable of receiving an e-mail. The system of claim 248 further includes software capable of detecting an access event; upon detecting such an access event, the software prompts the party associated with the access event to input recipient data before allowing the requested access. Such recipient data includes identifying data related to the party associated with the requested access. The system of claim 248 also includes a "means" for sending identifying data relating to the party associated with the access event to identify the party who accessed the e-mail.

As was noted above in regard to claim 236, Flynn does not prompt a recipient to input any recipient data that identifies the recipient. Flynn merely allows a requesting party to access the message, notes the email address to which such message is downloaded following such request, and notifies the sender of the email address to which such e-mail message was downloaded. The Examiner does not even contend, within Paragraph 3 of the Office Action, that Flynn prompts a party requesting access to input recipient data before permitting access to an e-mail message, as required by claim 248. Once again, Paragraph 3 of the Office Action fails to support the Examiner's rejection of claim 248 for obviousness based upon Choi, Flynn and Kanevsky.

Claim 252

As amended, claim 252 recites a system for verifying whether e-mail received by a recipient was accessed by an intended recipient. The system of claim 252 includes a recipient computer

connected to a communications network and capable of receiving an e-mail. The system of claim 252 further includes biometric identification means for recognizing biometric attributes of an individual. The system of claim 252 further includes software capable of detecting an access event and identifying an individual associated with the access event by using inputted biometric attributes of such individual. The software permits such e-mail to be accessed by the individual after such individual inputs biometric attributes of the individual associated with the access event.

The Examiner has already conceded that neither Choi nor Flynn disclose or suggest that an individual requesting access to an email input any biometric attributes of such individual. For this reason, the Examiner now relies upon Kanevsky.

Kanevsky describes a remote authentication process wherein the sender of an e-mail assigns an identity verification requirement (e.g. biometric identification) to such e-mail. Upon receipt of such e-mail, the receiving party must identify himself/herself via a biometric attribute such as a fingerprint scan. That biometric data is then communicated back to the sender of the e-mail. The returned biometric data is processed by doing a query in the sender's database. If the returned biometric data is verified against the sender's database, then the sender can grant to such recipient access to the original message by sending a further message granting such access (see Kanevsky specification at col. 6, lines 1-26).

Kanevsky also describes a local authentication process wherein the sender of an e-mail assigns an identity verification requirement (e.g. biometric identification) to such e-mail, along with expected authentication data. Upon receipt of such e-mail, the receiving party must identify himself/herself via a biometric attribute such as a fingerprint scan. That biometric data is then compared locally on the recipient's computer with the expected authentication data packaged with such e-mail message by the sender. The biometric data input by the person requesting access is compared to the expected biometric data packaged with the message by the sender. Only if they match is the person requesting access permitted to access such e-mail message (see Kanevsky specification at col. 6, lines 27-47).

In summary, Kanevsky teaches a method for authenticating the identity of the party requesting access of an e-mail by verifying their identity before allowing access to the e-mail. If the recipient's identity is not that of the intended recipient, then access to the e-mail is altogether denied by Kanevsky's system. In other words, Kavensky ensures that the recipient intended by the sender is the only party that can access the e-mail. On the other hand, the Kanevsky system cannot identify persons requesting access who are not the recipient intended by the sender, nor will it allow them access to such e-mail.

Even if it were "obvious" to modify Choi and/or Flynn, as the Examiner contends, to incorporate the teachings of Kanevsky, which Applicant does not concede, such a combination would nonetheless fail to achieve the system claimed in Applicant's claim 252. In the system of Applicant's claim 252, all parties requesting access to an e-mail (both intended and unintended) may access the e-mail, provided that they first input their biometric attributes to be identified. In other words, access to the e-mail is not conditioned upon whether the identity of the party requesting access is verified by the sender of the e-mail. The system recited by claim 252 allows all recipients access to the e-mail, but positively discovers the identity of the person requesting access, via biometric attributes, before the requesting party gains such access. The system of claim 252 is much less complicated, and more practical, than the system taught by Kanevsky.

The difference between the system of claim 252 and the system disclosed by Kanevsky might best be illustrated with the aid of an example. Suppose that a sender of an e-mail message is attemtping to send a message wherein the intended recipient is generally the "accounting" department of a company. In this case, it is likely that several employees working in the "accounting" department would be authorized to access e-mail messages sent to the general "accounting" mailbox of the company. All that would be important to the sender is to confirm that someone working at the firm's "accounting" department accessed the e-mail message, along with an identification of that person. Using the system of claim 252, anyone in the accounting department of the company could open the e-mail, and as a result, the identity of the accessing

party can be confirmed. In contrast, using the Kanevsky system, only a designated recipient would be able to access the e-mail; other un-designated individuals, who would otherwise be able to handle the incoming e-mail, would not be able to access to it.

Thus, the system recited by claim 252 would not be obvious even if one were to modify the Examiner's proposed combination of Choi and Flynn in accordance with the teachings of Kanevksy.

Claims 260, 264, 268

Claim 260 recites a method for verifying whether e-mail received by a recipient was accessed by an intended recipient, and includes, among other things, the steps of detecting an access event; acquiring recipient data that is related to biometric identification of the recipient; and permitting the e-mail to be accessed after acquiring such recipient data.

Claim 264 recites a method for verifying whether e-mail received by a recipient was accessed by an intended recipient, including, among other things, the steps of identifying a recipient utilizing biometric identification; detecting an access event; and permitting the e-mail to be accessed after acquiring such biometric identification.

Claim 268 recites a method for verifying whether e-mail received by a recipient was accessed by an intended recipient, and includes, among other things, the steps of identifying a recipient in association with biometric identification; detecting an access event; and permitting the e-mail to be accessed after acquiring such biometric identification.

Each of claims 260, 264 and 268 describes a method wherein a party requesting access to an e-mail must first provide biometric identification information, and wherein the requested access is permitted once the biometric identification information is acquired. For the same reasons explained in conjunction with claim 252 above, the Examiner's proposed combination of Choi, Flynn, and Kanevsky fails to achieve the methods recited by claims 260, 264 and 268.

Accordingly, each of independent claims 236, 248, 258, 260, 264, and 268 defines subject matter that would not have been obvious to those skilled in the art based upon the cited patents to Choi, Flynn and Kanevsky. Since these independent claims recite patentable subject matter, those claims dependent therefrom do as well.

Claim 258

The Examiner has imposed a separate rejection of independent claim 258 and claims 184, and 332-334 dependent therefrom, as describing subject matter considered obvious under Section 103(a) from Choi and Kanevsky.

Claim 258 recites a method for verifying whether an e-mail received by a recipient was accessed by an intended recipient, the method including, among others, the steps of detecting an access event; prompting the party that requested such access to input recipient data prior to allowing the requested access, and permitting the party requesting access to access the e-mail after that party inputs such recipient data. Claim 258 also recites that the recipient data which the requesting party is prompted to input includes identifying data associated with the requesting party.

Once again, the Examiner has conceded in the Office Action (see paragraph 14) that Choi does not disclose either: 1) detection of an access event; 2) prompting the requesting party to input recipient data before allowing access to an e-mail. However, the Examiner argues that Kanevsky supplies these missing features.

On the other hand, claim 258 includes the step of "permitting said e-mail to be accessed after the party that requested said access inputs said recipient data". As Applicant has already pointed out above, Kanevsky does not disclose a method for permitting access to an e-mail to any party that requests access merely because such party inputs recipient data. In the remote authorization method disclosed by Kanevsky, information provided by the party requesting access must first be sent to the sending party, processed through the sender's database, and another message must be sent to either authorize or deny access to the message. Even in the local

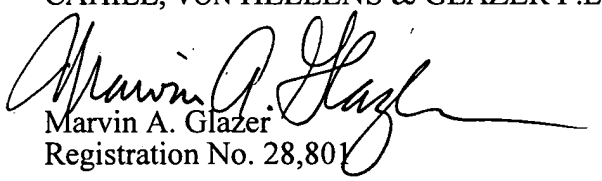
authorization method disclosed by Kanevsky, access is denied if the "recipient data" input by the party requesting access does not match the authorization information packaged with such e-mail message by the sender.

Accordingly, even if it were obvious to combine Kanevsky with Choi in the manner proposed by the Examiner, the result would still fail to provide the method recited by claim 258. Therefore, claim 258 and dependent claims 184, and 332-334 should be regarded as presenting patentable subject matter.

In view of the foregoing arguments, Applicant respectfully submits that all of the pending claims are allowable. Given the long and tortured prosecution of the present application, and the exhaustive searches of the prior art conducted by the Examiner, Applicant requests that the Examiner issue a prompt Notice of Allowance.

Respectfully submitted,

CAHILL, VON HELLENS & GLAZER P.L.C.



Marvin A. Glazer
Registration No. 28,801

155 Park One
2141 East Highland Avenue
Phoenix, Arizona 85016
Ph. (602) 956-7000
Fax (602) 495-9475
Docket No. 6589-A-7